

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Les relations contractuelles Banques - Entreprises entourant la mise à disposition de services télématiques bancaires

Amory, Bernard; Pouillet, Yves

Published in:
Electronic Banking

Publication date:
1989

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Amory, B & Pouillet, Y 1989, Les relations contractuelles Banques - Entreprises entourant la mise à disposition de services télématiques bancaires. Dans *Electronic Banking*. Précis de la Faculté de droit de Namur , Numéro 7, Story Scientia, Bruxelles, p. 29-57.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Les relations contractuelles banques-entreprises entourant la mise à disposition de services télématiques bancaires

Yves POULLET

*Chargé de cours aux
Facultés Universitaires de Namur
et Directeur du Centre de Recherches
Informatique et Droit des
Facultés Universitaires de Namur*

et

Bernard AMORY

*Assistant aux
Facultés Universitaires de Namur et
Membre du Cabinet juridique
Dechert Price & Rhoads,
Bruxelles*

Sommaire

1. Introduction	31
2. Les services télématiques offerts par les banques aux entreprises	31
2.1. Les techniques d'accès	31
2.2. Les services	32
2.2.1. Les services proprement bancaires	33
2.2.2. Les services non proprement bancaires	33
3. L'approche juridique des services télématiques bancaires	34
3.1. Règlement général, contrat-cadre et/ou dispositions spécifiques	34
3.2. La mise en route du service	34
3.2.1. Les dispositions relatives aux logiciels et aux matériels du client	35
3.2.2. La normalisation des messages	37
3.2.3. La nomination d'un correspondant technique	38
3.2.4. Les moyens d'accès	38
3.3. Le service	39
3.3.1. La disponibilité du service	39
3.3.2. L'envoi du message	40
3.3.3. La réception du message	41
3.3.4. L'exécution du message	41
3.4. Particularités relatives aux services non directement liés à une opération bancaire	42
3.4.1. Les purs services d'information	43
3.4.2. Les services de télétraitement	45
3.4.3. Les services de télétransaction	46
3.4.4. Conclusions	46
3.5. Les litiges relatifs aux services d'Electronic Banking	47
3.5.1. Preuve et 'signature'	47
3.5.2. Modes de règlement des litiges	52
3.5.3. Dommages et clauses d'exonération	52
Bibliographie	56

1. Introduction

La conjonction d'un matériel informatique de moins en moins coûteux et de plus en plus performant, l'existence de réseaux de transmission de capacité de plus en plus grande et de plus en plus sûrs ont permis l'éclosion de services télématiques financiers de plus en plus variés offerts aux entreprises.

Certes, la demande reste incertaine selon des études commerciales et les promoteurs de ces services. Ceux-ci y voient cependant outre l'avantage d'une image de marque 'nouvelles technologies' une manière de fidéliser la clientèle en offrant des services tantôt de simples informations, tantôt permettant l'accomplissement d'opérations financières.

L'objet des présentes réflexions porte d'une part, sur l'examen des dispositions contractuelles entourant l'offre et l'utilisation de ces services et, d'autre part, l'étude de certains problèmes fondamentaux qu'ils soulèvent: preuve, signature et responsabilité.

2. Les services télématiques offerts par les banques aux entreprises

Cette première partie décrit:

– d'une part, les techniques (dans leurs aspects matériels et logiciels) informatiques et de télécommunications nécessaires à la réalisation des opérations dites d'Electronic Banking' (point 2.1.);

– d'autre part, les divers services envisagés cette fois sous l'angle de leur contenu, et susceptibles d'être obtenus dans le cadre de telles opérations. On appréciera la diversité des services et l'ingéniosité mise par certaines banques à réaliser de nouveaux produits qui comme nous le verrons ne sont pas toujours directement liés à des opérations bancaires proprement dites (point 2.2.).

2.1. Les techniques d'accès

L'accès à un service télématique bancaire se réalise suivant différentes techniques. Une première distinction sépare les techniques d'accès en temps réel ('on-line') et celles en temps différé ('off-line'). Seules, les premières retiendront notre attention. Elles présentent l'avantage de permettre un dialogue interactif avec la base de données: l'utilisateur a l'occasion de préciser ses questions, les réponses affichées à son écran peuvent lui suggérer des nouvelles demandes de précision; enfin et surtout, l'intérêt de nombreux services télématiques bancaires se définit par la possibilité d'un accès immédiat, permettant des décisions instantanées (consultation de comptes, achats de titres, etc.).

La technique d'accès en temps réel nécessite une connexion au réseau de télécommunication. Il est rare, sauf pour certaines grosses entreprises, que l'accès aux services télématiques bancaires justifie à lui seul une ligne à usage privé c'est-à-dire une ligne louée. Dès lors, l'accès se fera via le réseau commuté public, réseau télex rarement, réseau téléphonique en mode analogique ou réseau par paquets, en attendant l'instauration des réseaux à large bande du type R.N.I.S., qui permettront des synthèses voix images.

Quant à la connexion elle-même, elle se réalise par différents 'modems', les critères de choix étant essentiellement la compatibilité avec l'équipement de l'utilisateur et la vitesse de transmission nécessaire.

L'équipement de l'utilisateur en logiciel et matériel mérite également quelques commentaires. Le choix par la banque de faire tourner les applications, qui permettront l'utilisation des services télématiques bancaires, sur tel type de programme, entraîne pour l'utilisateur, la nécessité des logiciels compatibles. Les contrats exigent souvent que ces logiciels soient agréés par la banque ou choisis parmi une liste proposée par celle-ci (cf. *infra*).

Cette dépendance à l'égard de la solution adoptée par le fournisseur de service (la banque, mais également son propre fournisseur de logiciel), et l'actuel manque de normalisation dans les choix de banques sont parfois considérés comme des freins au développement de la télématique bancaire, étant donné le coût que représenterait, pour des entreprises, la connexion avec leurs différentes banques.

Dès lors, certains plaident pour la généralisation du 'vidéotex bancaire'. Le principal intérêt du vidéotex est le faible coût de l'équipement (terminaux, carte interface). Il obligerait les banques à une normalisation de leur offre et se ferait selon une programmation simple. La solution vidéotex ne convient cependant qu'à des applications limitées pouvant néanmoins suffire pour des petites et moyennes entreprises.

2.2. Les services

Les services dont il est question dans la présente étude sont connus sous les noms de 'services télématiques financiers pour entreprises', 'services financiers et bancaires électroniques', 'télématique financière' ou 'Electronic Banking'. En l'absence d'une terminologie généralement reconnue en cette matière, nous les désignerons par l'expression 'services bancaires électroniques'.

Ces services constituent l'étape la plus récente du processus d'automatisation des banques visant à accélérer le mouvement des paiements et à en comprimer le coût.

Ce processus d'automatisation s'est d'abord développé au sein des banques elles-mêmes sur un plan purement interne (par exemple le télétraitement en agence bancaire). Ensuite, le phénomène s'est étendu aux relations interbancaires (par exemple, S.W.I.F.T.). Il restait à automatiser les relations entre les banques et leurs clients pour aboutir à un circuit électronique complet. Cette étape a été franchie, en ce qui concerne la clientèle 'grand public', avec l'installation des guichets automatiques de banques

et des terminaux points de vente (Cf. *supra* le rapport de MM. TROBERG et TRINQUET sur l'informatisation des rapports à la clientèle grand public) et, en ce qui concerne la clientèle 'entreprises', qui nous intéresse plus particulièrement dans le cadre de la présente étude, avec le développement des services bancaires électroniques pour entreprises. Une étape intermédiaire consiste en le transport physique de supports informatiques (par exemple des disquettes magnétiques) entre les clients et leurs banques, plutôt qu'un transport par télécommunications.

Quel est l'objet des services bancaires électroniques?

Il serait aventureux de prétendre en dresser une liste exhaustive, étant donné que l'imagination des banquiers conjuguée avec les innombrables possibilités offertes par l'informatique et la télématique donnent sans cesse naissance à de nouveaux services. Nous tentons néanmoins de dresser une liste des services les plus courants. Parmi ceux-ci, il y a lieu de distinguer pour la clarté de l'exposé, d'une part les services proprement bancaires et d'autre part les services non proprement bancaires.

2.2.1. Les services proprement bancaires

Parmi les services qui ont typiquement été offerts sous une forme non électronique par le secteur bancaire aux entreprises, il en est qui sont maintenant offerts également sous forme électronique. Il s'agit plus particulièrement:

- de la consultation immédiate par le client au moyen d'un terminal de l'état de ses comptes dans l'ensemble des filiales et succursales de la banque, le cas échéant à un niveau mondial, avec des possibilités supplémentaires comme celle d'obtenir un relevé des dernières opérations effectuées; à cette fin, certaines banques mettent leurs techniques à la disposition de leurs clients pour obtenir l'état de leurs comptes, dans d'autres banques ne disposant pas (encore) de services similaires (moyennant l'accord de ces autres banques et des précautions de confidentialité);
- de la transmission d'ordres de paiements, par exemple par virements et ce, non seulement, vers d'autres comptes du titulaire du service mais aussi vers des tiers;
- de l'ouverture de crédits documentaires;
- de la transmission d'ordres d'achat et de vente de valeurs mobilières.

2.2.2. Les services non proprement bancaires

Aux services mentionnés ci-dessus sont associés une multitude de services non proprement bancaires. On se reportera au point 3.4 pour leur description.

3. L'approche juridique des services télématiques bancaires

3.1. Règlement général, contrat-cadre et/ou dispositions spécifiques

Quelles sont les dispositions qui réglementent les services télématiques bancaires? On les trouve à trois niveaux. D'abord, dans le règlement général des opérations qui régit les rapports de la banque et ses clients de manière générale et sous réserve de dispositions contraires résultant de conventions ou règlements particuliers. Il est rare de trouver des dispositions propres aux services télématiques bancaires dans le règlement général des opérations. Toutefois, il est conseillé de veiller à ce que son contenu ne soit pas en contradiction avec la nature même des services télématiques bancaires. Les dispositions auxquelles on sera particulièrement attentifs sont celles relatives à la signature, à la formulation des ordres et à la conservation des documents à titre de preuve. Souvent les règlements généraux des opérations ont été rédigés bien avant l'apparition de la télématique bancaire d'où proviennent parfois des contradictions malheureuses entre leur contenu et les pratiques des banques.

Le deuxième niveau de réglementation des services télématiques bancaires est celui d'un contrat-cadre sous forme de règlement, convention ou simple lettre de la banque à son client, dans lequel sont régies les particularités des services télématiques bancaires. Leur objet est de définir les droits et obligations de la banque et de son client dans leurs rapports télématiques. L'importance d'un tel contrat ressort clairement de l'ensemble de cet exposé.

Il existe un troisième niveau de réglementation possible et celui-ci se situe au sein de l'échange télématique lui-même. En effet, les parties, la banque et son client, ont la possibilité d'échanger des messages sur leurs terminaux respectifs. Cette technique de correspondance leur permet de conclure des contrats, éventuellement, de déroger aux règlements généraux des opérations ou au contrat-cadre de services télématiques financiers. Si les parties usent de cette faculté, elles concluent un nouveau contrat. Mais de façon plus générale, on peut se demander (notamment par analogie avec les principes adoptés en matière d'ouverture de crédit) si chaque opération télématique ne doit pas être considérée comme un contrat particulier et non une simple exécution du contrat de services télématiques bancaires.

Dans l'affirmative, les conséquences sont importantes. En effet, de tels contrats seraient des 'contrats télématiques', c'est-à-dire des contrats conclus à distance au moyen des techniques de l'informatique et des télécommunications, ce qui soulève les délicates questions de l'authentification des parties à de tels contrats et de la preuve de ceux-ci. Ces questions sont abordées ci-après.

3.2. La mise en route du service

Préalablement à la mise en route du ou des services, certaines précautions apparaissent utiles de façon à prévenir des difficultés.

Ces précautions contractuelles envisagent:

- toutes les questions liées à la nécessité de logiciels et matériels compatibles avec le système choisi par la banque et au respect des directives de normalisation des messages;

- la nomination d'un responsable ou plutôt d'une personne de contact pour tous les problèmes techniques rencontrés lors de l'exécution des services;

- la remise des codes d'accès.

Les autres se limiteront à agréer une liste de programmes et de matériels susceptibles d'être connectés à leurs systèmes et de fournir les services, objet de la convention de télébanking.

3.2.1. Les dispositions relatives aux logiciels et aux matériels du client

Le bon fonctionnement des services télématiques bancaires suppose une possibilité de dialogue entre le système du client et celui de la banque. Ainsi, suivant le type d'ordinateur et de programmes de traitement choisi par la banque, le choix des programmes à installer dans l'ordinateur du client, voire le choix de son ordinateur pourront ne pas être libres. Cette remarque vaut tant pour les services relatifs à des opérations strictement bancaires que pour ceux relatifs à des opérations connexes (par exemple un logiciel de bases de données). Il est certain que ces exigences seront moins strictes si les services adoptent des normes générales, telle une des normes VIDEOTEX (Prestel - Minitel, etc.) et que dans le futur, on peut espérer une meilleure compatibilité entre les différentes configurations, notamment par l'adoption des normes I.S.O. pour les réseaux et d'operating systems' standards (UNIX) pour les équipements informatiques.

Ces remarques techniques proposées, il faut noter que les politiques des banques divergent: les unes proposent à leurs clients de leur fournir, sous licence, un ensemble original de programmes, dont elles assumeront elles-mêmes ou par l'intermédiaire de maisons spécialisées la maintenance; les autres laissent ce choix au client sous réserve d'une certaine agrégation de la part du banquier ou d'un tiers mandaté à cette fin.

a. Fourniture des programmes par la banque ou un tiers

Il est important alors de prévoir par un contrat séparé dit de licence de programmes, la possibilité pour le client de se servir du programme. Ce même contrat garantira à la banque ou au tiers concepteur du programme qu'aucune violation de leurs droits de propriété intellectuelle ne sera le fait du client (par exemple: droit limité d'utiliser le programme sur tel ordinateur en connexion avec le réseau, clauses d'interdiction de non-divulgaration et de copie de la documentation et du code-objet).

Un contrat de maintenance complétera le contrat de licence. Le maintien des fonctionnalités des services télématiques bancaires peut dépendre de l'évolution de la configuration. Ainsi, certaines dispositions réglementaires peuvent imposer l'adaptation de programmes. D'autre part, la correction d'erreurs de programme ou l'adjonction

de nouveaux services peuvent justifier l'intervention de programmeurs de la banque ou de tiers.

Dans l'hypothèse où les programmes sont livrés par des tiers, il est utile que la banque s'assure de la signature préalable de ces contrats comme condition à l'utilisation de ces services. En outre, il est utile qu'elle prévoit le consentement exprès du client à la communication d'informations même confidentielles nécessaires aux tiers pour assurer le bon fonctionnement du système.

Dans l'hypothèse où la banque détermine elle-même l'équipement et en particulier les programmes, qui devront être utilisés par le client, il apparaît difficile qu'elle puisse se dégager de toute responsabilité au cas où un vice de fonctionnement apparaîtrait comme le laisse entendre la clause suivante:

'Nous ne pouvons être tenus responsables pour le fonctionnement correct des équipements ou logiciels fournis par nous, ni des dommages de quelque nature qui en résulteraient, sauf en cas de négligence grave ou de faute intentionnelle de notre part'.

Certes, la banque peut subordonner une action en responsabilité contre elle à certaines conditions, ainsi, l'existence de mesures d'audit et de sécurité au sein de l'entreprise cliente, condition prévue par certaines conventions anglo-saxonnes et l'obligation d'une information immédiate en cas de défaillance dans le fonctionnement du système.

Enfin, il est clair que la banque conditionnera le maintien de la convention au respect de ses instructions et à la conclusion des contrats de maintenance ad hoc.

b. Fourniture des programmes par le client lui-même

Dans cette seconde hypothèse, le client acquiert lui-même l'équipement nécessaire. La fourniture des services télématiques peut se faire alors sous la condition suspensive de l'agrément par la banque de l'équipement choisi par le client ou de la conformité de l'équipement acquis aux spécifications techniques émises par la banque et généralement annexées à la convention.

Les agréments doivent viser l'équipement originaire, mais également les modifications rendues nécessaires par l'évolution de la configuration bancaire, comme il a été noté ci-dessus. Ainsi, l'acquisition d'une nouvelle configuration centrale, ou la modification de l'«operating system» par la banque peuvent affecter le fonctionnement des services et justifier des modifications de programme.

A ces sujets, on note les clauses suivantes:

'Le client déclare que les supports informatiques qui sont utilisés par lui dans le cadre de la présente convention répondent aux spécifications techniques précisées en annexe... de la présente convention...'

'Les spécifications précitées peuvent être modifiées à tout moment par la banque notamment, en vue d'améliorer le service et ce, moyennant préavis de X jours'.

'Préalablement à la mise en fonctionnement du service et en cas de modification des spécifications techniques, la Banque peut soumettre l'équipement du client à un test de conformité'.

L'agrément par la banque n'est pas toujours prévu, comme l'atteste une autre convention:

'Le client est responsable de l'installation et de l'utilisation de son matériel dont les caractéristiques doivent être compatibles avec les spécifications fournies par la Banque'.

S'il est clair que le non-respect des procédures d'agrément ou de conformité des équipements entraîne une présomption d'irresponsabilité de la banque, il est plus délicat d'en conclure qu'à l'inverse les défaillances prouvées d'un équipement agréé ou conforme sont à charge du banquier. Celui-ci ne pourrait, nous semble-t-il, être tenu qu'au cas où un bon conseiller savait ou devait savoir le risque attaché à l'utilisation de tel équipement en connexion avec tel autre équipement.

3.2.2. La normalisation des messages

La normalisation administrative des messages, c'est-à-dire leur présentation conforme à une certaine structure, que celle-ci soit imposée par une banque, un groupe de banques (ex.: les normes TRASEC établies par l'Association belge des banques), une agence réglementaire ou quasi réglementaire (ex.: les normes du Centre d'échange et de compensation à Bruxelles) ou un transporteur privé (ex.: S.W.I.F.T.), poursuit différents buts:

- elle permet une circulation aisée des messages d'un organisme financier à l'autre sans obliger à un décodage-réencodage, supprimant par là même des risques d'erreurs de transcription;

- elle permet la mise au point de logiciels de sécurité vérifiant automatiquement la séquentialité des messages, leur structure et leur correspondance aux normes afin de détecter des erreurs ou fraudes.

Il est donc indispensable que des mesures de normalisation des messages transmis par le donneur d'ordre soient prévues à peine de refuser l'exécution des ordres non normalisés reçus ou en tout cas de s'exonérer de toute responsabilité à leur propos. Ainsi, tout ordre de paiement comprendra suivant un ordre strict, le nom du donneur d'ordre, le nom du bénéficiaire, etc... De plus, il sera affecté d'un numéro séquentiel et des totaux partiels devront être effectués à des fréquences déterminées,...

Il est indispensable à nouveau que la banque puisse revoir, moyennant préavis, ces mesures de normalisation, soit à raison de l'évolution de ses propres programmes, soit à raison de l'action d'autres organes de normalisation.

'La Banque se réserve le droit de modifier l'ensemble des consignes, moyennant préavis d'un mois, après communication au client des modifications envisagées et des conséquences possibles sur la programmation'.

En ce qui concerne la valeur juridique de la normalisation, en particulier dans le domaine interbancaire, ajoutons à la suite de Bruyneel que 'le juge y trouvera l'expression de la manière dont un bon banquier... se comporte aujourd'hui; il en déduira la norme de comportement et, partant, le critère de faute que constitue cette norme et sa violation'. Ainsi, les procédures standardisées seront peu à peu absorbées par le droit sous forme d'inclusion dans les standards de bon comportement.

3.2.3. La nomination d'un correspondant technique

Il est indispensable de prévoir, en raison des difficultés techniques qui pourraient survenir lors de l'exécution des opérations, de nommer une ou deux (en cas d'absence du premier responsable) personne(s) de contact dans l'entreprise cliente. Cette (ou ces) personne(s) sera (seront) seule(s) habilitée(s) à prendre des décisions lors de tels événements.

'Le client désigne M... et, en son absence, M... comme responsables techniques qui peuvent être contactés par la Banque au ... pour toute difficulté technique relative au fonctionnement du service'.

3.2.4. Les moyens d'accès

L'accès automatique aux comptes de l'entreprise et la possibilité immédiate d'ordonner des mouvements sur le compte, qu'autorisent les services télématiques financiers, justifient les précautions prises par les banques et les entreprises dans la remise des moyens d'accès.

La procédure d'octroi des moyens d'accès et le choix du numéro personnel d'identification ('P.I.N.') sont le fait de l'entreprise. Celle-ci certifie alors à la banque les noms des différents titulaires des moyens d'accès, leurs fonctions dans l'entreprise, le montant pour lesquels ils sont autorisés seuls ou conjointement à effectuer des transactions au nom de l'entreprise.

Le numéro personnel d'identification est choisi par les membres du personnel ainsi désignés. La plupart des systèmes permettent aujourd'hui une modification automatique du numéro voire obligent régulièrement à certaines modifications.

L'entreprise peut à tout moment suivant certaines procédures modifier la liste des personnes autorisées à effectuer des transactions. Elle garantit que tous les membres du personnel autorisés connaissent et acceptent les mesures de sécurité imposées par la banque, voire atteste de l'existence et des conclusions d'un audit relatif à la sécurité technique de l'ensemble de l'équipement de l'entreprise.

A l'octroi de ces mots de passe, correspondent des obligations à charge des entreprises.

'Le client et les employés autorisés prendront toutes les mesures nécessaires pour éviter que des tiers ou des employés non autorisés puissent avoir accès à la connaissance de tout ou partie de la procédure, des règles de sécurité, du (ou des) moyen(s) d'identification, ainsi que de toute information sur le fonctionnement du système pouvant revêtir un caractère confidentiel.'

A cette obligation de confidentialité s'ajoute par voie de conséquence, la responsabilité de l'entreprise pour toutes les conséquences directes et indirectes de l'utilisation par des tiers ou des personnes non autorisées, qui pourrait être faite du système, du moyen d'identification et de la procédure.

'Please be advised that we will consider any access to the system using a valid profile and correct corresponding password to be made by the individual to whom the profile has been assigned, and we will carry out any instructions given within the authorized password of that individual regardless of the true identity of the individual physically at the terminal'.

En contrepartie de ces obligations mises à charge de l'entreprise, la banque devrait s'engager à rendre effectives dans un délai déterminé, voire immédiatement, les modifications demandées par l'entreprise, c'est-à-dire par exemple de bloquer tout ordre de paiement qui serait le fait d'une personne dont l'entreprise a signalé le retrait d'autorisation. Elle s'engage également à mettre sur pied un certain nombre de mesures de sécurité, ainsi garder en mémoire l'identification des émetteurs d'ordre de paiement et le terminal à partir duquel ils ont agi; prévenir l'entreprise de l'existence d'un certain nombre d'essais d'utilisations non autorisées du service, etc.

3.3. Le service

Il importe de définir les modalités du service. Quatre aspects retiendront notre attention: la disponibilité du service, l'envoi, la réception et l'exécution des messages.

3.3.1. La disponibilité du service

Si, par définition, les services télématiques bancaires sont susceptibles d'offrir une plus grande disponibilité de la banque à l'égard de son client, il ne faut pas en conclure qu'ils permettent toujours une disponibilité totale (24 heures sur 24). Des impératifs techniques (par exemple l'entretien des systèmes) y font obstacle. Il faut que le client soit informé du temps de disponibilité exacte. On conseille de prévoir dans le

contrat-cadre une clause (éventuellement renvoyant à une annexe) précisant les heures d'ouverture du service.

'Les services sont en principe accessibles chaque jour bancaire ouvrable de ... heures à ... heures. L'accessibilité aux services peut être interrompue pour raison d'entretien des systèmes de la banque, pour y effectuer des réparations nécessaires et y apporter des améliorations. Sauf en cas d'urgence ou raison de sécurité impérieuse, la banque avertit le client de toute interruption des services prévisible au moins deux jours bancaires ouvrables à l'avance'.

Une telle clause n'aura cependant qu'une valeur indicative et il sera prévu que le service pourra être interrompu en cas de travaux visant à son amélioration ou en cas de réparations nécessaires et en raison de tout événement indépendant de la volonté de la banque.

3.3.2. L'envoi du message

Les personnes autorisées auxquelles ont été remis des codes d'accès (voir ci-dessus) sont les seules à pouvoir effectuer l'envoi du message par télécommunication à son destinataire. C'est au moment de cet envoi que peuvent naître des problèmes d'authentification, de signature et de risques de transmission, bien que ces problèmes ne se révéleront qu'en cas de litige (voir ci-après).

Le client doit authentifier son message, c'est-à-dire donner à la banque l'assurance que le message émane bien de lui et qu'il a marqué son accord sur son contenu et ce, étant donné la technique utilisée, sans recours à la signature manuscrite. Le message risque d'être perdu ou altéré en cours de transmission. Qui de la banque ou du client supportera ce risque étant donné qu'un recours contre le transporteur public (les P.T.T.) est exclu dans la plupart des pays?

Dans les contrats entre absents, l'expéditeur est en principe responsable du choix du moyen de transmission. Il n'est pas sûr que cette règle serait applicable dans les cas où la banque imposerait un système de transmission à son client.

Enfin, c'est aussi au moment de l'envoi du message qu'il faut constituer les moyens de preuve qui devront éventuellement être utilisés en cas de litige. Les parties conviendront utilement de la valeur probante des documents informatiques relatifs à l'envoi du message.

'Le journal des instructions reçues (le 'logging') par la banque en conséquence de l'utilisation des services, lequel peut être visualisé sur papier, sur microfilm ou sur microfiche, constitue la preuve des ordres donnés par le client. La procédure d'identification équivaut à la signature du client par laquelle il reconnaît être l'auteur des instructions enregistrées sur le logging et marque son accord sur leur contenu'.

On soulignera cependant que la clause relative à la preuve ne peut pas ôter à une partie la possibilité de contester la véracité des documents dont il est convenu qu'ils font preuve des opérations effectuées (voir ci-après discussion relative à la preuve).

3.3.3. La réception du message

Opération parallèle à l'envoi, la réception du message suscite les mêmes questions que celles examinées ci-dessus, questions qui resurgissent en cas de litige. La banque ne peut donner suite à un message que si elle est sûre que ce message émane bien de celui qui prétend être son auteur et qu'il lui est parvenu tel qu'il fut envoyé. Les règles de l'apparence (mandat apparent par exemple) n'exemptent pas la banque de toute vérification. En effet, la banque serait responsable si elle donnait suite à un message qui était manifestement affecté d'erreur ou de fraude. On remarquera que l'automatisation rend ce genre de contrôle difficile. La banque devra également se constituer des moyens de preuve du message reçu, à utiliser en cas de litige.

3.3.4. L'exécution du message

On distinguera deux questions: les délais d'exécution et les opérations d'exécution.

— Les délais d'exécution

La publicité faite par les banques à propos des services télématiques bancaires porte le plus souvent sur la rapidité des opérations qu'ils permettent. Le client peut donc s'attendre à ce que le service soit plus rapide que lorsqu'il est effectué sans recours à la télématique. Il peut toutefois être dangereux pour la banque de s'engager à respecter un délai fixé à l'avance, étant donné que des contraintes tant externes à la banque (par exemple: disponibilité des lignes de télécommunication) qu'internes à celle-ci peuvent entraîner des retards.

Si des délais d'exécution sont prévus, par exemple pour des ordres de virements transmis par télécommunication, il y a lieu de distinguer les ordres pouvant être exécutés de façon interne à la banque, et ceux nécessitant de passer par une chambre de compensation. En ce qui concerne ces derniers, la banque ne peut être tenue qu'à un délai de présentation en chambre de compensation des ordres transmis.

En cas d'engagements de la banque sur les délais, ceux-ci seront assortis de réserves. Aux réserves classiques portant sur les cas de force majeure (y compris panne du réseau bancaire ou du transporteur, grève du personnel, ...) doivent être ajoutées des réserves spécifiques à l'opération, ainsi celles de la vérification des clés d'accès et, de façon générale, toutes les procédures de contrôle et de sécurité prévues au contrat. On peut aussi prévoir l'obligation pour la banque d'avertir le client au cas où une détérioration du système ne lui permettrait plus de remplir ses engagements.

– Les opérations d'exécution

Trois principes doivent être mis en évidence: le principe de la confiance, le principe de la non-immixtion et le principe de l'auto-satisfaction.

Le *principe de la confiance* signifie que la banque accepte les messages reçus du client et n'a à en vérifier ni la véracité, ni la plausibilité, en d'autres termes, qu'elle accepte comme tels les messages reçus selon la procédure prévue et qu'elle les exécute tels quels. Son seul devoir (comparativement avec la solution en matière de crédit documentaire) est de vérifier que les messages reçus sont conformes aux procédures formelles mises au point en accord avec le client.

Au cas où de telles vérifications ne pourraient être effectuées ou feraient apparaître l'existence d'une erreur ou d'une fraude, le second principe serait appelé à jouer.

Le *principe de la non-immixtion* signifie d'abord que si lors de l'exécution d'un message, une procédure de vérification ne peut aboutir, la banque s'interdit de modifier les informations reçues et ne leur donne pas suite. Son obligation est alors d'avertir dès que possible le client. Le principe signifie ensuite qu'en cas de demande de modification d'un message déjà reçu (par exemple parce que le client découvre l'existence d'une erreur dans un numéro de compte après avoir envoyé le message), le banquier demandera au client de corriger lui-même le message (ou à l'y autoriser).

Le troisième principe est celui de l'*auto-satisfaction*. Il est utile que le banquier puisse se prévaloir, en cas de contestation sur le déroulement des opérations et d'erreur soupçonnée, d'une preuve '*prima facie*' de sa bonne exécution des opérations. Dans cette optique, le client devrait reconnaître expressément que le logging de la banque constitue une preuve formelle et suffisante des messages reçus du client.

3.4. Particularités relatives aux services non directement liés à une opération bancaire

La connexion par téléinformatique avec une banque permet à son client d'obtenir bien d'autres services que ceux constituant strictement un mode de réalisation d'une opération bancaire, ou ayant trait aux opérations bancaires.

De nombreux promoteurs de services télématiques bancaires affirment que le succès de leur produit tient en partie, voire essentiellement, à cette possibilité pour l'entreprise cliente d'avoir accès à d'autres services et que les opérations effectuées, grâce à la mise en place de la connexion téléinformatique, concernent principalement de tels services.

Les services envisagés sont de divers ordres:

– il s'agit, d'abord, des services d'accès à des bases de données généralement distribuées, rarement produites, par les banques;

– il s'agit ensuite, des services de *télétraitement* joints ou indépendants des services d'information préalablement cités. Ainsi, certaines banques couplent l'accès à des bases de données bilantaires et la possibilité d'appliquer à ces bases, certains traitements, tel le calcul des ratios comptables, etc. Les mêmes banques ou d'autres permettent aux entreprises de procéder en temps réel à certains traitements de leurs propres données. On pourrait songer ainsi au calcul de certains préavis, au calcul de rentabilité de certains placements ou investissements, etc.

– enfin, on songe à des services de *télétransaction*, telle, la réservation automatique de billets d'avion.

Si les services annexes représentent indiscutablement une importante valeur ajoutée et, en tant que tels, font parfois l'objet d'une facturation séparée, peu de conventions relatives aux services télématiques bancaires préviennent les problèmes qui risquent de naître à l'occasion de l'utilisation de ces services annexes.

Le présent chapitre entend proposer quelques réflexions à leur sujet, dans la mesure où il s'agit de problèmes spécifiques soulevés par l'utilisation de ces services.

3.4.1. Les purs services d'information

Le service d'accès à des bases de données produites par la banque elle-même ou par des tiers mais distribuées par la banque fait rarement l'objet de clauses spécifiques.

On citera l'une d'elles:

'La Banque n'est pas responsable du contenu des bases de données, autres que celles relatives au compte du client auquel le système permet d'accéder. La Banque ne peut en aucun cas être tenue responsable de l'adéquation des informations à un besoin particulier du client, ainsi que des conséquences de l'utilisation du client de ces données.'

La responsabilité relative au *contenu* de la base, c'est-à-dire, relative aux différents aspects (caractère complet, mise à jour, convivialité, qualité de l'indexation) qualitatifs des produits informationnels auxquels l'utilisateur aura accès, nous semble pouvoir s'analyser différemment si le banquier est le 'producteur' ou simplement le distributeur du produit informationnel envisagé. Ainsi, simple distributeur et pour autant que le banquier le stipule clairement en indiquant le réel producteur, le banquier ne peut être tenu responsable d'obligations relatives au contenu des bases de données. Producteur, il pourrait l'être par contre, si les qualités de la base de données ne correspondent point à celles décrites dans la documentation y relative ou à défaut de documentation explicite, à celle que l'on peut normalement attendre d'un fournisseur d'informations diligent, et ce, en fonction du type-même de bases de données produites.

Dans les hypothèses exceptionnelles où la faute du banquier pourrait être retenue, il restera à l'utilisateur à faire la preuve du préjudice et du lien de causalité. Le principe suivant lequel: 'Plus le sens du conseil et de son objet correspondait à une nécessité pour celui-ci et plus aisément le juge y verra la cause de l'aide ou de l'abstention du

client' ne peut être appliqué ici. En effet, la délivrance automatique d'informations par le biais d'un service télématique ne permet pas une individualisation consciente des besoins du client, ce qui est le propre du contrat de conseil.

On ajoutera que des clauses conventionnelles limitant a priori le dommage causé par l'information absente, incomplète, fausse sont parfaitement pensables, ainsi, celles fréquentes dans les contrats utilisateurs relatifs à l'accès aux bases de données et stipulées comme suit:

'Bien que... et les différents producteurs des banques de données disponibles n'aient aucune raison de penser qu'il y ait des inexactitudes ou des défauts dans les informations ou services fournis, ils ne donnent aucune assurance ni garantie explicite ou implicite concernant, notamment, l'appropriation du service à un usage quelconque.

Le client accepte de dégager... de toute responsabilité à l'égard des dommages indirects ou fortuits, des pertes de profits et de toute action en réparation ou revendication de nature quelconque formulée contre ... ou contre le client par un tiers du fait des services ou des matériaux fournis dans le cadre de l'accord ou de leur utilisation. Le client s'engage à garantir et mettre à couvert... contre toute action en réparation intentée par des tiers par suite de l'utilisation qu'il fera des services ou des matériaux fournis dans le cadre du présent accord.'

On ajoutera que l'information obtenue ne supprime ni la liberté de l'utilisateur de s'informer ailleurs, ni celle de décider de son attitude finale.

Distributeur du produit informationnel, le banquier sera souvent appelé à offrir deux garanties supplémentaires, l'une, au producteur, l'autre, à l'utilisateur.

Vis-à-vis des producteurs, il s'engagera à imposer aux utilisateurs finaux les restrictions d'utilisation de la base de données et assurera le respect des 'Downloading Policies' réclamées par les producteurs pour protéger la rentabilité de l'investissement que constitue la mise sur pied d'une base de données.

Ces restrictions d'utilisation seront annexées au contrat de télébanking et constitueront partie intégrante de ce contrat.

Le même souci amènera la banque, lorsqu'elle est elle-même producteur de bases de données à insérer dans son contrat des clauses relatives à l'utilisation de ses propres produits informationnels.

A cet égard, on note la clause suivante:

'Le client en particulier prendra toutes les mesures de sécurité et les fera prendre auprès de ses préposés pour le respect du caractère secret ou confidentiel de toutes les informations commerciales qui devront être traitées aussi discrètement que possible, et qui seront indiquées comme telles.'

Vis-à-vis des utilisateurs, le serveur peut s'engager ensuite à assurer la confidentialité de leurs interrogations et des réponses obtenues par eux, même vis-à-vis des producteurs:

'La Banque s'interdit de communiquer à des tiers les données dont elle peut avoir connaissance du fait de l'exécution des présentes. Les seules exceptions à ce principe trouvent leurs causes dans les lois et la réglementation applicables aux banques' (par exemple: droit de communication des administrations, des autorités de tutelle, éventuellement déclarations ou contrôle des organismes chargés d'assurer le respect des réglementations de protection des données).

3.4.2. Les services de télétraitement

Par un service de télétraitement, la banque met à disposition de ses clients, son équipement informatique et certains de ses programmes, afin d'appliquer aux données que lui confie le client, un traitement et de lui fournir un produit final utilisable.

Ainsi en annexe d'un service 'infobilians' la banque peut offrir un service permettant le calcul de certains ratios comptables, voire de détecter certains indicateurs de faillite, dans le cadre de systèmes-experts ou de systèmes d'aide à la décision.

La mise à disposition par les banques de services de télétraitement, en particulier de systèmes d'aides à la décision, nécessite certaines précautions. Les réflexions qui suivent concernent principalement de tels systèmes.

Il est bien évident que l'utilisateur sera sensible plus encore que dans le cadre de services de pure information, aux obligations de confidentialité des données résultant de l'utilisation de tels services.

Cependant, c'est principalement vis-à-vis des conséquences dommageables de l'utilisation des systèmes d'aide à la décision que certaines clauses dans les contrats de services financiers électroniques sont nécessaires. Chacun imagine aisément de telles conséquences. Une entreprise, sur base du jugement négatif proposé par le système-expert, relatif à la solvabilité d'un de ses clients, prendra la décision de rompre ses relations contractuelles avec ce client, ou prendra, sur le conseil d'un système d'aide à la déclaration fiscale, une décision, qui par la suite, s'avérera inopportune.

Il est donc utile que la banque avertisse clairement, par des clauses appropriées, son client des précautions à prendre avant l'utilisation de ces services de télétraitement. Des clauses rappelant les limites et la responsabilité ultime du client dans la décision finale sont utiles, et leur rappel sur la page écran précédant le service est à conseiller. De même, il est intéressant de rendre transparentes à la demande du client les règles logiques retenues pour la confection du système-expert et de restreindre l'utilisation de certains de ces systèmes à certaines personnes formées par la banque.

Ceci dit, la banque reste responsable pour les erreurs dues à l'opérateur ou au logiciel non fourni par le client, lorsque ce dernier peut apporter la preuve que l'erreur n'a pas été causée par ses propres données ou ses programmes.

Enfin, la mauvaise qualité intrinsèque du programme, c'est-à-dire l'inadéquation ou le caractère incorrect des règles retenues par rapport au problème à solutionner pourrait engager la responsabilité de son auteur, d'autant plus que celui-ci se présente comme expert. Certes, il ne peut garantir que dans toutes les hypothèses concrètes, l'application du programme donne un résultat fiable, encore faut-il que la constitution

de son programme réponde aux règles de l'art, c'est-à-dire à ce qui peut être attendu d'un bon expert du domaine d'application considéré.

3.4.3. Les services de télétransaction

La diversification des activités bancaires a amené certaines banques à proposer, dans le cadre de services nouveaux, tels ceux d'agences de voyages, des services de télétransaction.

Comme pour les services de télétraitement, il n'existe pas de clauses particulières à ces services dans les contrats actuels de services d'Electronic Banking. Or, le même besoin de prévenir les incidents particuliers à ces services existe.

Des précautions techniques et, notamment, le système d'écho rappelant la demande du client et réclamant confirmation de cette demande sont à notre avis nécessaires lors de la mise sur pied de tels services. Il suffit de rappeler ici le principe déjà mis en évidence pour les services de transactions bancaires selon lequel le banquier est responsable de la technique qu'il propose. Normalement, il lui impose de mettre au point un système techniquement fiable et offrant les garanties préventives minimales nécessaires.

La référence à ces précautions techniques renforcera la valeur de la clause conventionnelle relative à la preuve des transactions effectuées dans le cadre de l'utilisation de tels services. La clause reprendra la clause générale déjà établie à propos des services électroniques financiers et suivant laquelle:

'Les parties reconnaissent que le journal des transactions effectuées ('le logging'), établi par la banque, en conséquence de l'utilisation du service, lequel peut être visualisé sur papier, sur microfiche ou sur microfilm, constitue une preuve formelle et suffisante des ordres donnés par l'abonné et ce quel qu'en soit le montant.'

3.4.4. Conclusions

L'importance des services télématiques offerts par les banques et non directement liés à des opérations bancaires appelle quelques aménagements des contrats d'Electronic Banking.

a. Il serait utile, étant donné la *spécificité de ces services* et des problèmes juridiques qu'ils posent, que des dispositions contractuelles spécifiques régissent leur mise à disposition et s'ajoutent à certaines dispositions générales relatives à l'ensemble des services (code d'accès, preuve, fonctionnement du service, etc.).

b. Ces dispositions spécifiques devraient s'inspirer des *clauses relatives à ces services lorsqu'ils sont l'objet principal d'un contrat* conclu avec une entreprise spécialisée; ainsi pour l'accès à des bases de données, il serait utile de reprendre certaines clauses relatives à la responsabilité du contenu des données, aux restrictions d'utilisation et aux obligations de confidentialité des données d'interrogation.

c. Une *facturation séparée* de ces services et des *modalités particulières de résiliation ou d'accès* sont également souhaitables. Il est utile que le client identifie clairement le coût d'utilisation de ces services et que la *résiliation de tels services présentés comme annexes* n'affecte pas la totalité de la relation contractuelle.

3.5. Les litiges relatifs aux services d'Electronic Banking

D'une part, le client qui se plaint de l'inexécution ou de la mauvaise exécution par le banquier de ses obligations et, d'autre part, la banque qui prétend souffrir d'un dommage du fait du client ou entend prévenir de tels dommages, peuvent rencontrer quelques difficultés à obtenir justice, du fait de la spécificité des services d'Electronic Banking.

- La dématérialisation des opérations, principale caractéristique de ces services, entraîne une difficulté de prouver la réalité des opérations. Le problème de la preuve et de la signature fera donc l'objet de clauses spécifiques.

- Le mode de règlement des litiges peut également être particulier du fait de la technicité des questions soulevées.

- Enfin, le dommage subi par l'une ou l'autre des parties peut être difficile à évaluer: certaines clauses particulières peuvent le circonscrire ou l'étendre; les causes de ce dommage peuvent être multiples, étant donné la multiplicité des intervenants et la technique utilisée. Ici également, des clauses d'exonération de responsabilité peuvent préciser les causes imputables à chacune des parties.

3.5.1. Preuve et 'signature'

Notre propos n'est pas de reprendre une étude exhaustive et doctrinale de la valeur juridique des moyens de preuve électronique, et de la 'signature' électronique au regard des exigences légales en la matière. Il s'agit ici d'analyser les clauses à ce sujet, présentes dans les contrats de télébanking et de poser un certain nombre de principes à leur sujet.

Deux remarques préalables introduiront le sujet:

1. La présence de ces clauses est automatique dans les conventions émises par les banques d'Europe continentale. Elle est moins évidente chez nos voisins d'Outre-Manche et d'Outre-Atlantique. Sans doute, est-ce précisément, l'existence d'exigences légales à propos de la preuve et de la signature qui justifie dans nos pays d'Europe continentale ces précautions contractuelles.

2. Certaines conventions distinguent les clauses relatives à la 'signature' et celles relatives à la preuve. En fait, preuve et 'signature' ne sont que deux facettes d'un problème plus large: celui de l'authentification des documents. L'authentification revêt en effet trois fonctions:

1. Démontrer l'existence et le contenu d'un message;
2. Identifier la personne qui en est l'auteur;

3. Indiquer sa volonté de s'approprier le contenu du message.

Par clause relative à la 'signature', les conventions entendent généralement les clauses répondant aux deux dernières fonctions de l'authentification, les clauses relatives à la 'preuve' concernant la première fonction.

La distinction des deux types de clauses peut être utile, l'objet de la contestation n'étant pas le même dans les deux cas. Ainsi, le client, sans contester être l'auteur de la transaction peut simplement contester le montant de celle-ci.

a. Clauses relatives à la 'signature'

'Il est expressément convenu que la procédure d'accès aux services, telle qu'elle a été définie à l'annexe... et communiquée au client, sera considérée par les deux parties comme preuve valable et irréfutable de l'identité et de l'accord des parties pour toutes les instructions données sous couvert de cette procédure.'

Le principe selon lequel l'utilisation du numéro d'identification et du protocole vaut signature mérite d'être discuté. Nous proposons à cet égard trois réflexions : la première s'interroge sur la légitimité de l'utilisation du terme 'signature' ou 'signature électronique' à ce propos; la deuxième confronte la solution conventionnelle affirmée ci-dessus et la solution jurisprudentielle habituellement retenue en matière de virement; enfin, la troisième propose une analyse des limites de validité d'une telle clause.

Sur le premier point, il nous apparaît que la notion de 'signature' doit être réservée à une expression de la personnalité de l'individu par laquelle celui-ci marque son adhésion au contenu d'un document. Un moyen technique d'identification de l'émetteur d'un message même présentant toutes les caractéristiques de fiabilité ne peut être assimilé à une 'signature', au sens légal du terme. Il représente un moyen d'authentification reconnu comme valable entre les parties dans le cadre d'une convention par ailleurs signée; ce moyen d'authentification est dès lors recevable par le juge en vertu du principe de l'autonomie contractuelle, pour autant qu'aucune règle de droit public n'impose une signature.

Si les parties peuvent donc entre elles se satisfaire pour la preuve de leur adhésion à un acte juridique, d'un simple moyen d'authentification, reste posée la question de l'opposabilité à une partie d'un ordre 'authentifié' mais n'émanant pas de la partie à qui on l'oppose. Les hypothèses visées sont celles du 'vol' par un tiers du moyen d'authentification ou de l'erreur technique ou humaine dans la lecture par le banquier du moyen d'authentification.

En matière de virement-papier, la solution proposée par la jurisprudence met en principe à charge du banquier mandataire la responsabilité de l'exécution de virements effectuée sur ordres faux ou falsifiés. En pareils cas, la banque, même si aucune faute ne peut lui être reprochée (par exemple imitation de signature), n'a en effet pas reçu mandat de son client, le pseudo-donneur d'ordre. On sait que la solution est différente en matière de chèques et de lettres de change où la loi n'impute la responsabilité au banquier qu'en cas de faute lourde ou de dol. Ce régime d'exception légale ne peut cependant en aucune manière être étendu au cas du virement électronique.

Ceci dit, premièrement, en dehors de toute clause, en cas de contestation par le soi-disant donneur d'ordre de l'utilisation par lui du code confidentiel, le juge pourra exiger que celui-ci étaie sa contestation. Il est clair que l'utilisation d'un numéro secret d'identification laisse présumer que l'ordre émane bien de celui qui a reçu le numéro secret.

En second lieu, nonobstant les moyens de preuve apportés par le donneur d'ordre présumé, le juge pourra souvent au nom de la théorie du mandat apparent, mettre à charge du titulaire du numéro secret la responsabilité de l'ordre, celui-ci ayant vraisemblablement commis une faute dans la garde de son numéro.

A supposer que le donneur d'ordre présumé non seulement renverse la présomption mais en outre démontre l'absence de toute faute dans la garde du numéro d'identification, le juge peut-il, en fonction du seul principe de la liberté contractuelle, condamner le soi-disant donneur d'ordre, la clause discutée affirmant qu'irréfragablement, l'ordre est présumé émaner de ce dernier? C'est l'objet de notre troisième réflexion.

Il nous semble que la clause conventionnelle ne peut, en tout cas, équivaloir à une renonciation a priori par le client de la banque à contester en justice les ordres de virement qui lui sont attribués. Certes, la preuve lui sera difficile, elle n'est cependant pas impossible. En vertu du principe du devoir de collaboration des parties à l'établissement de la preuve, au cas où le donneur d'ordre établit à suffisance la vraisemblance que l'ordre n'émane pas de lui, le juge pourra exiger que le banquier fasse la preuve de la parfaite sécurité de son système. Le juge sera attentif aux procédures de délivrance des numéros secrets, à la déontologie du personnel et aux techniques de sécurité qui définissent la signature électronique (par exemple l'utilisation de techniques de cryptographie à clés asymétriques, de préférence à des techniques symétriques ou de simples numéros d'identification).

En résumé, telle que rédigée, la clause nous apparaît mélanger trois problèmes différents et qu'il serait peut-être utile de distinguer:

a) la clause établit bien qu'entre parties, l'utilisation du code d'accès, du P.I.N. (1) et le respect des procédures est une technique d'authentification suffisante, valable entre parties;

b) la clause peut également en outre stipuler que l'utilisation des protocoles et les procédures rappelées ci-dessous constituent une présomption de 'signature';

c) la clause peut enfin stipuler que le client étant contractuellement responsable de la garde et de la confidentialité de ces moyens d'accès, il est tenu en cas de non-respect de cette obligation de garde, des conséquences de leur utilisation.

Une telle sanction de la faute contractuelle pourrait être appliquée sauf, pour l'utilisateur, à démontrer qu'étant donné le contenu du message (par ex.: message aberrant) ou l'attitude du client (par ex.: le client avait signalé le risque), il y a eu faute de

(1) Personal Identification Number.

la banque de ne pas avoir mis sur pied ou appliqué les procédures de sécurité nécessaires dans ces hypothèses.

A cet égard, on note que le même contrat que celui contenant la clause-type citée en exergue stipule la clause suivante:

'Le client reconnaît être pleinement et inconditionnellement responsable de l'usage abusif, étranger à la Banque, qui pourrait être le fait du système, du moyen d'identification et de la procédure. Il déclare assumer l'entière responsabilité des conséquences tant directes qu'indirectes découlant de cet emploi abusif.'

b. La preuve

La clause-type est la suivante:

'Le client accepte sans réserve que les ordres soient transmis et exécutés conformément aux données enregistrées par la Banque. Il reconnaît les données enregistrées par la Banque comme conformes, correctes, exactes et contraignantes pour toutes les parties. Lorsqu'il prétend qu'il y a eu faute ou erreur dans le fonctionnement du système, le client doit en fournir la preuve. Sous peine de perdre tous ses droits, le client doit introduire sa réclamation écrite auprès de la Banque dans les 15 jours suivant la date de l'opération concernée.'

Il est indéniable qu'une convention relative aux moyens de preuve est parfaitement licite. Ainsi, conformément à la clause précitée, par la convention-cadre à la base de toutes les opérations nées des utilisations du service télématique, les parties conviennent de donner force probante aux données codées reprises sur les supports magnétiques de la banque et le juge devra, conformément à ladite convention des parties recevoir le moyen de preuve prévu par les parties.

Le client peut-il pour autant s'interdire de contester un tel moyen de preuve, comme le laissent entendre la clause citée et certaines conventions parlant de *'preuve formelle, suffisante et irréfutable'*?

Il nous apparaît que non et ce, pour les mêmes raisons que celles déjà avancées pour les clauses relatives à la signature. Une telle affirmation équivaldrait en effet à dénier tout droit du client à agir en justice. La clause citée elle-même répugne à en tirer une telle conclusion, puisqu'après avoir affirmé que les *'données enregistrées par la Banque...'* sont *'contraignantes'*, elle évoque la possibilité de preuve contraire, l'alinéa 3 spécifiant l'obligation d'agir dans de brefs délais, les 15 jours, durée probable de la conservation par la banque en mémoire des instructions données par ses clients. Nous reviendrons sur cette seconde partie de la clause citée.

Ainsi, une convention licite relative à la recevabilité des moyens de preuve ne peut aller jusqu'à donner une *force contraignante absolue* à un moyen de preuve. C'est sans doute le premier principe à évoquer en la matière.

Peut-on dénier à une partie la possibilité d'amener, nonobstant une clause conventionnelle, des moyens de preuve contraires?

Affirmer que le moyen de preuve ne constitue qu'une présomption de preuve et permet, dès lors, un renversement de la charge de la preuve, n'est-ce pas déjà répondre négativement?

La doctrine de tous nos pays européens admet qu'il est possible de limiter les droits de recours du contractant, notamment par des délais de forclusion, l'exclusion de certains moyens de preuve, etc., pour autant que ces limites n'équivalent pas pratiquement à une impossibilité pour le client d'agir.

Il n'empêche que saisi d'un litige, le juge pourra, suivant le principe de la collaboration des parties à la solution du litige, exiger la *production de documents*, ordonner une *expertise* sur la fiabilité des programmes et les procédures de sécurité internes à la banque, en même temps qu'il appréciera les moyens de preuve apportés par le client, (par exemple: copie sur l'imprimante du client des instructions données à la banque; conservation dans la mémoire du client, etc.).

En ce qui concerne la fiabilité des programmes et la sécurité des procédures, le juge s'inspirera le cas échéant, des principes de la recommandation n° R (81) du Conseil de l'Europe, adoptée le 11 décembre 1981 et plus particulièrement de l'article suivant:

'Art. 5.

1. Les règles suivantes s'appliquent aux programmes informatiques:

a) La documentation de programme, les descriptions de fichiers et les instructions de programme doivent être directement lisibles et tenues soigneusement à jour sous la responsabilité du commerçant ou de toute autre personne définie par la loi nationale.

b) Les documents définis à l'alinéa a) ci-dessus doivent être conservés sous une forme communicable aussi longtemps que les enregistrements auxquels ils se réfèrent.

2. Si, pour une raison quelconque, les données enregistrées sont transférées d'un support informatique à un autre, le commerçant ou la personne définie par la loi nationale doit démontrer leur concordance.

3. Les règles suivantes, aux systèmes informatiques dans leur ensemble:

a) Les systèmes doivent comporter les sécurités nécessaires pour éviter une altération des enregistrements.

b) Les systèmes doivent permettre de restituer à tout instant les informations enregistrées sous une forme directement lisible.'

Les alinéas 2 et 3 de la clause citée en exergue de nos réflexions sur la preuve suggèrent une *seconde question: peut-on circonscrire dans le temps la possibilité de recours du client?*

Une première remarque concerne le délai stipulé par la plupart des conventions: ce délai est calculé tantôt à partir de la réception de l'extrait de compte écrit, tantôt à partir de l'exécution de l'instruction et de son inscription au compte du client. Dans la mesure où la consultation des comptes peut être faite on line et la mise à jour de ceux-ci est immédiate, on peut concevoir que la distinction quant au point de départ du délai est sans relevance. Reste à savoir si le principe même d'une telle clause n'équivaut

pas à une obligation faite au client de consulter fréquemment ses comptes et à vérifier les écritures qui y sont portées.

La CNUDCI relève différents arguments en faveur de la thèse suivant laquelle le client doit examiner le relevé que lui envoie la banque. On note parmi ces arguments: *'Le relevé, et notamment le relevé périodique, peut être considéré comme une offre d'apurement du compte entre la banque et son client... Il est utile aux parties de s'accorder périodiquement sur l'état de leurs relations, de sorte qu'à la fin d'une période relativement longue, il ne soit pas nécessaire de vérifier chaque opération effectuée, longtemps après que les détails en aient été oubliés et que les traces en aient disparu'. 'Si l'on tarde à en informer la banque, il est plus difficile à cette dernière de rectifier la transaction ou de limiter la perte'.*

En l'espèce, les clauses citées apparaissent donc licites; elles se justifient par les nécessités du service: on ne peut imposer à la banque la charge de conserver indéfiniment la trace des instructions du client et l'obligation de donner suite à toute contestation du client, en contrepassant les instructions contestées et en bloquant toutes les instructions données depuis.

Il nous apparaît dès lors qu'à la suite de ces arguments, le principe de la clause est parfaitement défendable.

3.5.2. Modes de règlement des litiges

La plupart des conventions reprennent une clause classique d'attribution de juridiction aux tribunaux du lieu du siège de la banque et une clause d'applicabilité du droit du pays de la banque. Il est étonnant, étant donné, d'une part, les questions techniques que soulève souvent la solution des litiges, d'autre part, les nécessités de confidentialité et de rapidité qui caractérisent la solution des litiges, que les contractants ne songent pas à des modes alternatifs de résolution des litiges, tels l'arbitrage, voire le 'mini-trial'. Pour les mêmes raisons, ces procédures se sont développées en matière de litiges informatiques. On conçoit aisément, qu'elles pourraient s'appliquer à la résolution des litiges relatifs aux services de télébanking.

Plus étonnant encore, l'absence de clauses confiant à un ou des représentants de l'entreprise et de la banque la mission de rechercher une solution transactionnelle avant de porter le différend devant les tribunaux.

3.5.3. Dommages et clauses d'exonération

Ce dernier point entend examiner une des questions majeures posées par les conventions de télébanking. De quoi, en définitive, la banque peut-elle être tenue responsable?

La solution à la question suppose l'étude des clauses d'exonération de responsabilité nombreuses dans les conventions de télébanking. Elle nécessite d'abord l'identifica-

tion claire des risques liés à l'exécution d'une opération bancaire, tel un ordre de paiement ou de recouvrement et le rappel des principes en matière de responsabilité.

a. Les risques et dommages

La perte du montant principal (en tout ou en partie). Celle-ci peut se produire lorsqu'un transfert électronique est crédité à un compte qui n'est pas le bon, crédité au bon compte pour un montant excessif ou effectué deux fois, et que le bénéficiaire retire les fonds qu'il ne peut restituer.

La perte d'intérêts. Celle-ci résulte de retards apportés au transfert car certaines banques prétendant pouvoir transférer les fonds instantanément, leurs clients ont tendance à retenir l'ordre de transfert jusqu'au dernier moment.

Pertes dues aux taux de change. Celles-ci se produisent quand un retard dans le transfert est couplé à une fluctuation dans le taux de change.

On remarquera que les dommages mentionnés aux points 2 et 3 supposent pour leur évaluation que l'on puisse déterminer avec précision le délai dans lequel le transfert aurait dû être effectué.

Les dommages dits 'indirects', c'est-à-dire tous les dommages qui sont liés, soit à la spécificité de l'opération commerciale ou financière dont l'ordre de paiement ou de recouvrement représentait une exécution, par ex.: la perte de la possibilité de participer à une Chartepartie pour retard de paiement d'acompte, l'imposition d'une pénalité à charge du donneur d'ordre pour retard dans son paiement, soit à la situation d'une des parties, par ex. la faillite du donneur d'ordre conséquence d'un retard dans le recouvrement d'une créance.

Le dommage réparable

Avec des raisonnements sans doute bien différents, les droits continentaux et ceux anglo-saxons s'accordent pour affirmer que sont à réparer les dommages qui ont été prévus ou qui étaient raisonnablement prévisibles au banquier diligent, lors de la conclusion du contrat.

Dans la relation entre le banquier et son client, il est difficile de connaître a priori quels dommages sont prévisibles: si les trois premiers types de dommages le sont certainement, certains dommages dits 'indirects' peuvent l'être également. Ainsi, une entreprise peut avertir la banque des raisons qui justifient l'envoi d'un ordre de paiement et de la nécessité de respecter certains délais d'exécution. Ainsi, une banque peut, connaissant la situation financière délicate de son client, prévoir les conséquences dommageables du retard de paiement.

Les clauses d'exonération

Deux principes sont à noter: d'abord que nos droits continentaux et anglo-saxons *légitiment les clauses d'exonération de responsabilité*. Ensuite que, d'une part, en Angleterre, des législations spécifiques (Unfair Contract Terms Act, Misrepresentation Act), et d'autre part, dans les pays continentaux, des principes doctrinaux limitent la validité de certaines clauses d'exonération.

Notre propos n'est pas d'analyser doctrinalement le contenu de ces deux principes, mais d'étudier les hypothèses conventionnelles les plus fréquentes d'exclusion de responsabilité et d'en proposer la critique sur base du principe: est-il raisonnable d'admettre une telle exclusion?

On distinguera en ce sens, les clauses d'exclusion des responsabilités relatives:

- au fait du transporteur;
- au fait de tiers, en particulier des autres intervenants bancaires nécessaires à la bonne fin de l'opération initiée par le client;
- aux défauts de l'équipement (matériel et logiciel).

a. du fait du transporteur

L'exclusion par la banque de toute responsabilité pour fait du transporteur, y compris l'interception ou la déformation d'un message par un tiers pendant le transport est fréquente: *'La Banque ne pourra être tenue responsable des dommages et difficultés imputables au mauvais fonctionnement du réseau d'accès...'*

Une telle exclusion nous apparaît parfaitement légitime sous deux réserves:

Il est certain que la responsabilité de la banque doit être appréciée différemment lorsqu'il s'agit d'un réseau commuté public ou d'un réseau privé (lignes louées), sur lequel la banque peut implémenter toute mesure de sécurité quant à la circulation des messages.

Il est également évident que la banque doit prendre les *mesures minimales* nécessaires *quant à la sécurité des messages* (par ex. en implémentant des programmes cryptographiant les messages), de sorte à ne pas créer de risques évidents de lectures des messages par des tiers et à permettre un contrôle facile des manipulations de messages par des tiers non autorisés.

On ajoutera qu'à cette exonération du banquier s'ajoutera dans de nombreux pays celle totale ou quasi totale, du transporteur public. Le client risque donc de se trouver fort démuni.

b. du fait de tiers

L'inexécution envers un tiers domicilié dans une autre banque, peut résulter de la défaillance d'une banque intermédiaire, d'un organisme de compensation ou d'un organisme se chargeant du transfert du message tel S.W.I.F.T. Cette défaillance peut s'expliquer, soit par l'insolvabilité de ces intermédiaires, soit par leur négligence.

De façon générale, la banque ne garantit que ses propres services et non ceux des tiers, seraient-ils intervenus à sa demande.

En l'absence de disposition contractuelle spécifique, la banque du donneur d'ordre pourrait se voir reprocher par son client une *faute dans le choix des moyens* pour opérer le transfert, quitte à se retourner elle-même dans un second temps contre l'intermédiaire défaillant.

Cette responsabilité de la banque du donneur d'ordre pour le fait de ses sous-traitants ne peut, sauf à l'imposer par voie législative, équivaloir à une responsabilité 'pour tout le réseau', c'est-à-dire pour le fait de tous les intermédiaires devant intervenir pour la bonne fin de l'ordre donné.

En effet, à défaut de cette disposition législative, la banque du donneur d'ordre ne peut se voir reprocher une *faute de choix*, notamment:

- en ce qui concerne l'intervention des chambres de compensation;
- en ce qui concerne l'intervention de la banque du bénéficiaire;
- en ce qui concerne bien souvent, le transporteur interbancaire, soit que le client ait demandé le transit de son message par ce transporteur, soit de toute façon, que l'on puisse difficilement reprocher le choix de ce moyen plus sûr que les moyens de transfert traditionnel.

Il n'en reste pas moins que des clauses pourraient prévoir une exonération de responsabilité de la banque transférante en ce cas. Ces clauses sont valables en vertu du principe de la liberté des conventions (art. 1134 du Code civil).

L'utilisateur paraît démuni dans cette hypothèse puisqu'il est tiers par rapport au contrat qui lie la banque transférante et la banque intermédiaire.

Cette solution n'est cependant pas totalement satisfaisante: elle est discutable sur le plan théorique et elle aboutit en définitive à faire reposer le risque de l'opération sur le donneur d'ordre (ex: le recours contre une banque insolvable) et, de façon plus générale, à lui faire supporter le risque d'un mode de transfert qu'il n'a pas choisi et auquel il est extérieur. Que l'on songe au cas où le transfert n'a pas été effectué correctement et où il n'est pas possible, contrairement à l'hypothèse développée ci-dessus, de déterminer quelle est la cause du préjudice, chaque entité du système va affirmer que le problème lui est étranger, avec toutes les difficultés de preuve que cela implique pour le client.

Cette difficulté d'identification peut amener à prôner, de lege ferenda, la responsabilité pour l'ensemble de l'opération de la banque transférante, solution qui présente d'incontestables avantages pour l'utilisateur.

c. des défauts de l'équipement (matériel et logiciel)

'Il est précisé, autant que de besoin, que la Banque ne fournit aucune garantie expresse ou implicite en ce qui concerne l'aptitude du système à atteindre les objectifs de la présente convention.'

De nombreux contrats de télébanking exonèrent la banque explicitement ou implicitement de toute responsabilité au cas où celle-ci peut démontrer que la non-exécution, ou la mauvaise exécution, d'un ordre est due à une panne ou un mauvais fonctionnement du matériel ou du logiciel.

Les causes de pannes ou de mauvais fonctionnement sont multiples: panne d'électricité, erreur dans le logiciel, incompatibilité de matériel ou de programmes, mainte-

nance. Les pannes ou mauvais fonctionnements peuvent avoir des conséquences graves: perte de certaines instructions, déformation de messages, etc. La justification de la clause tient essentiellement au fait de la radicale imprévisibilité des pannes, au fait que bien souvent le logiciel est livré par un tiers.

De tels arguments ne peuvent remettre en cause le principe suivant lequel 'professionnel, le banquier répond de sa technique, il en répond, c'est-à-dire qu'il en est responsable, il en assume le risque...'. Ce principe met à charge du banquier une présomption de responsabilité en cas de mauvais fonctionnement du système: il ne pourra qu'exceptionnellement invoquer la faute d'un tiers dans la mesure où il avait à prévoir les procédures de sécurité nécessaires à la détection préventive des erreurs et des pannes. Ainsi, il se verra reprocher de ne pas avoir prévu de systèmes de back up, de programmes de contrôle de cohérence des opérations enregistrées et de blocage immédiat des opérations en cas de panne du système.

Bibliographie

B. AMORY et X. THUNIS, 'Authentification de l'origine et du contenu des transactions sans papier et questions de responsabilité en droit continental', exposé présenté lors de la Conférence sur 'Les Transactions commerciales Internationales assistées par ordinateur et droit dans la C.E.E.', organisée par C.E.L.I.M. à Bruxelles les 17 et 18 mars 1986, 43 et s.

B. AMORY et Y. POULLET, 'Le droit de la preuve face à l'informatique et à la télématique, Approche de droit comparé', *R.I.D.C.*, 1985, n° 2, 331 à 352.

E. BERGSTEN, 'E.F.T.: How can it influence the formation of contracts', in 'La validez de los contratos internacionales negociados por medios electronicos', Coll. Madrid, 3-4 mars 1987.

A. BRUYNEEL, 'Le virement', in *La Banque dans la vie quotidienne*, Ed. du Jeune Barreau, Bruylant, Bruxelles, 1985, 370-450.

J.T. BURNETT, *Information and the Law of Banking*, Paper, T.D.R. Conf., 30 octobre-1^{er} novembre 1985.

D. CARTON, 'Aspects juridiques des ordres de virement transmis par télex', D.I.S.E.P., octobre 1985, 4.

B. CRAWFORD, *Does Canada need a payment Code*, Can. Business Law Journal, 1982-83, 45-71.

CNUDCI, 'Projet de Guide juridique sur les Transferts électroniques de fonds', ACN9250 Add. 4, p. 25.

R. GOODE, *Electronic Banking*, London, 1986.

J. LASS, 'Electronic Banking: Formation of contracts - Legal Issues' in *La validez de los contratos internacionales negociados por medios electronicos*, Coll. Madrid, 3-4 mars 1987.

H.F. LINGL, 'Risk Allocation in International Interbank Electronic Fund Transfers: CHIPS and SWIFT', *Harvard Int'l Law Journal*, vol. 22, number 3, Fall 1981, 621-630.

S. MACCARONE, *L'elettronica nell'Attività Bancaria*, Soluzione Technique e problemi Giuridici, Roma, 15-16 déc. 1982, 31 pages.

C. PESCATORE, '30 ans de révolution bancaire: la monnaie électronique remplace la monnaie scripturale', dans la série 'Notes Economiques et Financières' publiée par le Crédit Européen S.A., Luxembourg, (1985).

Y. POULLET et X. THUNIS, 'Réflexions sur le mouvement électronique de fonds', in 'La Télématique', Story-Scientia, Gand (1985), tome 2, 259 et s.

Y. POULLET et G. VANDENBERGHE, 'Telebanking - Teleshopping: Legal Aspects', Research Report made for the Legal Observatory (D.G. XIII - EEC), March 87 (to be published).

H.S. SCOTT, 'Sur les transferts interbancaires par télétransmission aux Etats-Unis', *R.I.D.C.*, 4-1985, 967-984, v.p. 977-981.

D. SYX, 'Le transfert électronique de fonds: le droit hésitant face à une réalité galopante' in *La Télématique: aspects techniques, juridiques et socio-politiques*, Story-Scientia, Gand (1985), tome 2, 224-225.

D. SYX, 'Het bewijsrecht en de informatica: een verkenning van een recente problematiek', basistekst i.v.m. de cursus 'De computer en zijn toepassingsproblemen in het recht', les van 26 februari 1985, Faculteit Rechtsgeleerdheid, R.U.G., publié in *Droit de l'informatique*, 1986, n° 4.

M. VASSEUR, 'Aspects juridiques des nouveaux moyens de paiement', *Rev. Banque*, 1982, 580.

M. VAN QUICKENBORNE, 'Quelques réflexions sur la signature des actes sous seing privé', note sous Cass., 28 juin 1982, *R.C.J.B.*, 69 et s.